WIRESHARK BANDSTEERING

Filtro para encontrar tramas con 802.11v BSS Transition Management Requests y Responses:
wlan.fixed.action_code == 7 || wlan.fixed.action_code == 8

Enlace para descargar captura realizada y WLAN Pros Master v2 perfil para Wireshark:
https://www.dropbox.com/sh/lt4lgkmtytpewi9/AACndpnsTsT_zDt1D-b8Ipbea?dl=0

Y acá está la grabación de la sesión:
https://thewifiofthings.com/130a-sesion-de-tess-en-wi-fi-wlpc-medellin-bss-transition-mgmt-interferencia-5ghz-wireshark/

DOCUMENTO DE BSS IEEE.

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjEi5ql3IKEAxVdfjABHZ0TAfwQFnoECA8QAQ&url=https%3A%2F%2Fgithub.com%2FFCAE%2FWLAN%2Fblob%2Fmaster%2Fdoc%2F802.11-2012.pdf&usg=AOvVaw0AD2qBEda2pvRN8vm5Jay6&opi=89978449

((((wlan.fc.type_subtype == 0x00) || (wlan.fc.type_subtype == 0x01) || wlan.fc.type_subtype == 0x02 || wlan.fc.type_subtype == 0x03 || wlan.fc.type_subtype == 0x04 || wlan.fc.type_subtype == 0x05 || wlan.fixed.action_code==7 || wlan.fixed.action_code==8 || wlan.fc.type_subtype == 0x0B || wlan.fc.type_subtype == 0x0A)))&&(((wlan.sa==78:6a:1f:4f:48:00) && (wlan.da==16:fe:92:67:dc:e7)) || ((wlan.da==78:6a:1f:4f:48:00) && (wlan.sa==16:fe:92:67:dc:e7)))

https://zhuanlan.zhihu.com/p/472071741

wlan.fixed.bss_transition_status_code == 7

Then the more important is a BSS Transition Status Code. The value in the figure is 7. Check the protocol. 7 means: Reject-No suitable BSS transition candidates.
To sum up: AP sent a BSS Transition Management Request, suggesting that STA cut to another BSSID: 50:64:2b:b5:80:7e, but STA refused, believing that there

was no suitable candidates.

BSS Transition Management Response

相对来说，response帧的内容就少了很多，

```
> Frame 4525: 33 bytes on wire (264 bits), 33 bytes captured (264 bits)
> 802.11 radio information
> IEEE 802.11 Action, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters
      Category code: WNM (10)
      Action code: BSS Transition Management Response (8)
      Dialog token: 0x08
      BSS Transition Status Code: 7
      BSS Termination Delay: 0
```


直接看协议中的规定，如图：

	Category	WNM Action	Dialog Token	BTM Status Code	BSS Termination Delay	Target BSSID (Optional)	BSS Transition Candidate List Entries (Optional)
Octets:	1	1	1	1	1	0 or 6	variable

Figure 9-927—BSS Transition Management Response frame Action field format

Table 9-428—BTM status code definitions

Status code	Status code description
0	Accept
1	Reject—Unspecified reject reason.
2	Reject—Insufficient Beacon or Probe Response frames received from all candidates.
3	Reject—Insufficient available capacity from all candidates.
4	Reject—BSS termination undesired.
5	Reject—BSS termination delay requested.
6	Reject—STA BSS Transition Candidate List provided.
7	Reject—No suitable BSS transition candidates.
8	Reject—Leaving ESS.
9–255	Reserved

The client can answer to this transition request with a positive response. In this case the status code 0 means that this transition was accepted:

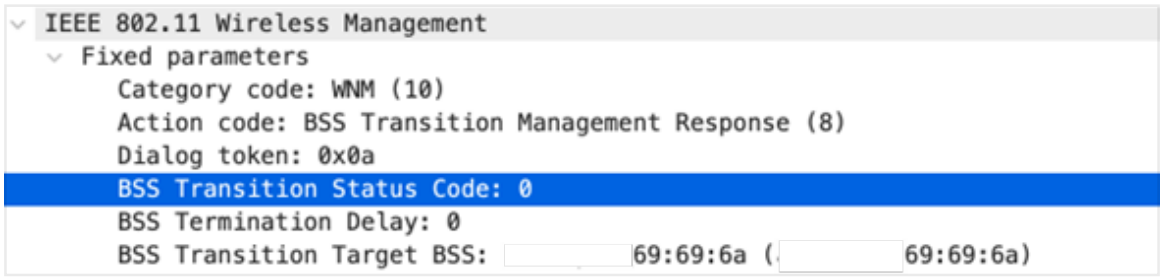


Image 4

https://www.cleartosend.net/cts-211-a-look-into-802-11v/
If the AP transmits a BSS Transition Management Request frame with the Disassociation Imminent field set to 1, the Disassociation Timer field in that Request frame will be set to 0 or set to the number of TBTTs that will occur prior to the AP disassociating the station.

Depending on what the station receives from the AP within the BSS Termination field, it will send a BSS Transition Management Response frame with a status code.
The status code can be any of the following, but Status Code 0 is an Accept:

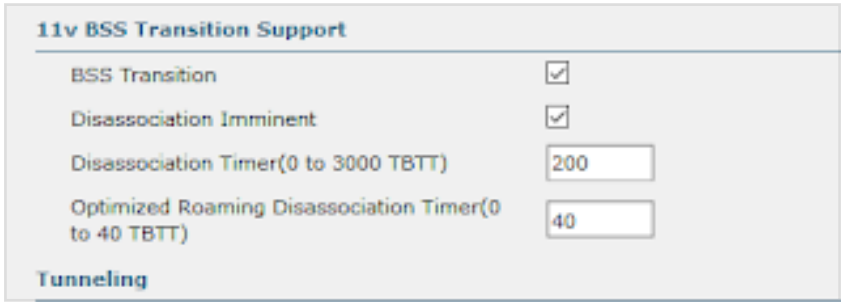
Wireshark Filters

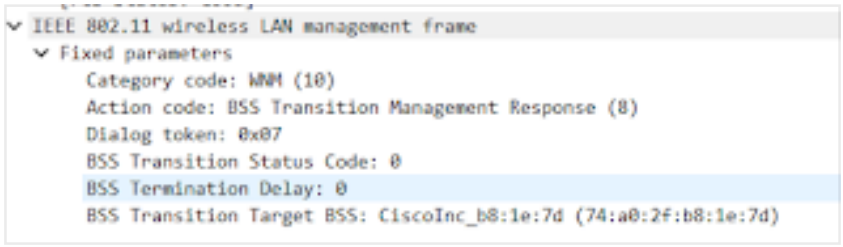
- Find out if my SSID supports 802.11v: wlan.extcap.b19 == 1
- Find all Wireless Network Management frames: wlan.fixed.category_code == 10
- Find BSS Transition Management Query: wlan.fixed.action_code == 6
- Find BSS Transition Management Request: wlan.fixed.action_code == 7
- Find BSS Transition Management Response: wlan.fixed.action_code == 8

https://mrncciew.com/2014/10/11/802-11-mgmt-deauth-disassociation-frames/

http://giantsnerdwifi.blogspot.com/2016/11/cisco-11v-bss-transition-management_7.html

The client responds with a BTM response frame, shown below.





The key items to look for here are that the "BSS Transition Target BSS" matches the BSSID given in the BTM request, and that the values for the Dialog token field match.

BSS transition management

802.11v BSS Transition Management Request is a suggestion given to client. Client can make its own decision whether to follow the suggestion or not. The disassociation of a client **can be forced if disassociation-imminent function is enabled**. It disassociates the client after **a period of time if the client does not re-associate to one of the suggested APs.**

802.11v BSS Transition is applied to these four scenarios:

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/201015-802-11v-Basic-Service-Set-BSS-on-AireO.html

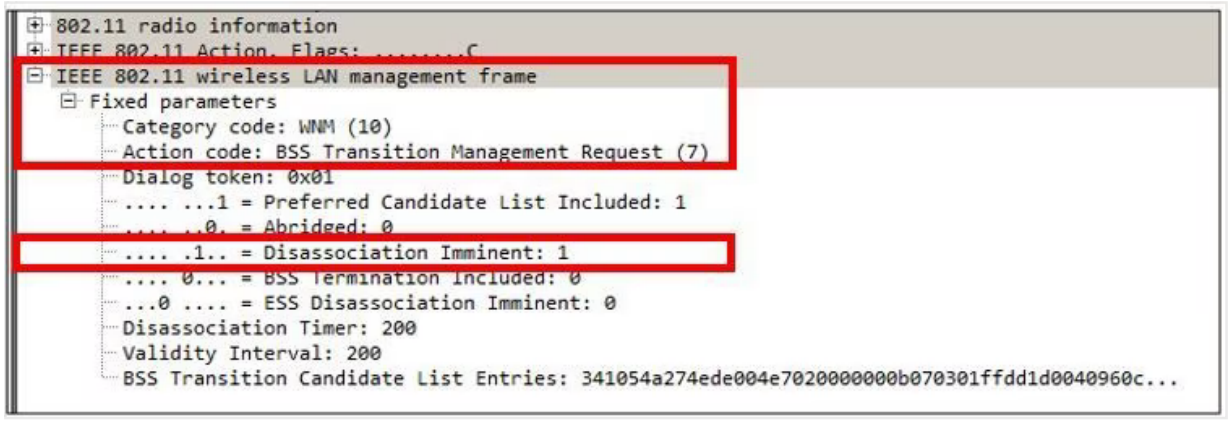
Disassociation Imminent

Within a BSS transition Management Request, Disassociation Imminent field can be added. This function is to disassociate the client after a period of time if the client does not re-associate to another AP.

When unsolicited optimized roaming request is triggered, the AP sends a BSS Transition Management Request to the client and wait for a certain period (time configured under Optimized Roaming Disassociation Timer), if the client does not roam to a better AP within that period of time, then the AP completes the disassociation of the client.

When Unsolicited Load Balance request is triggered, the AP sends a BSS Transition Management Request to the client and wait for a certain period (time configured under Disassociation Timer), if the client does not roam to a less congested AP within that period of time, then the AP completes the disassociation of the client.

Example of a BSS transition management frame with Disassociation imminent enabled:

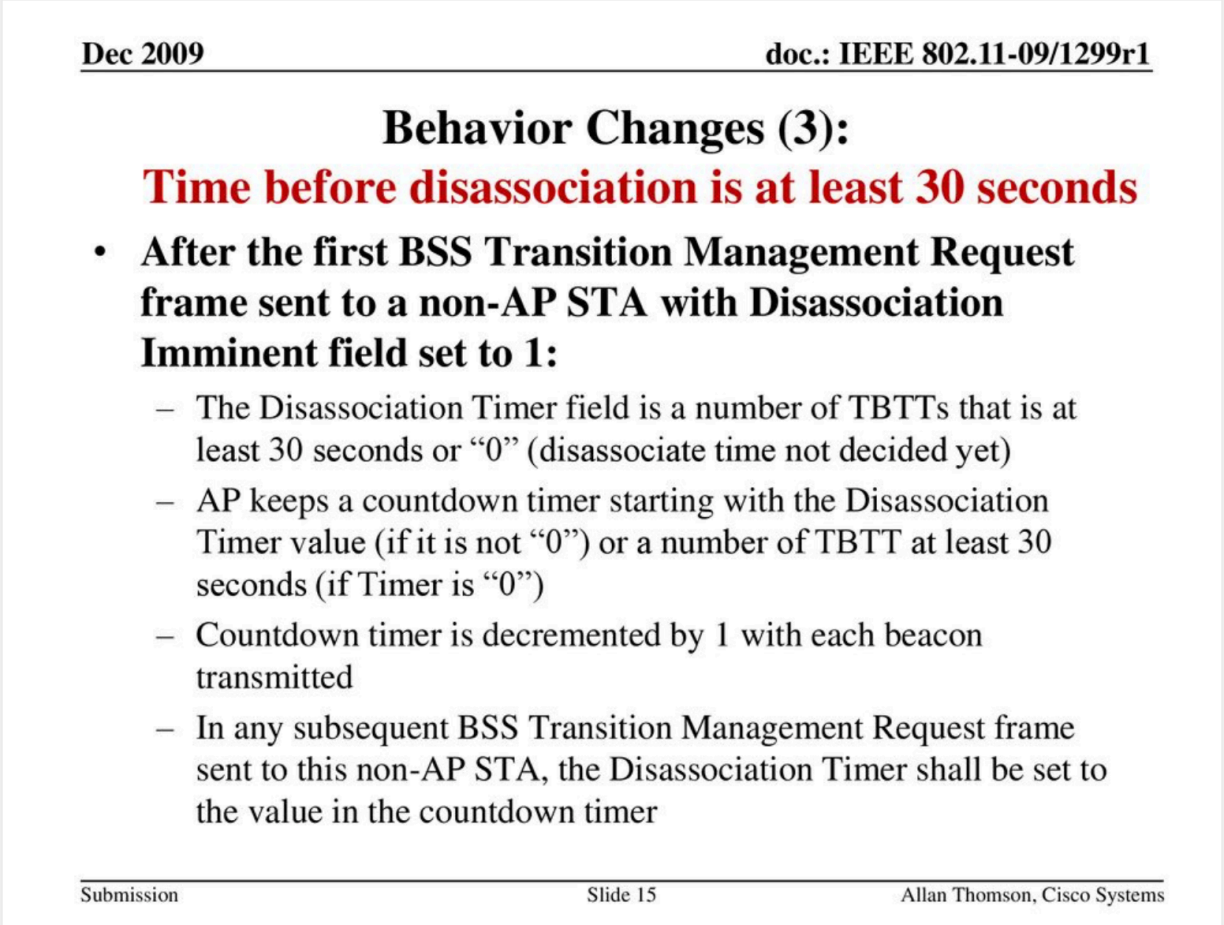


PILAS

The Disassociation Timer indicates the time after which the AP ~~issues~~sends a Disassociation frame to the STA or the AP affiliated with the AP MLD sends a Disassociation frame to the non-AP STA affiliated with this non-AP MLD. The Disassociation Timer field contains the number of beacon transmission times (TBTTs) until the AP sends a Disassociation frame to the STA or the AP affiliated with the AP MLD sends a

Disassociation frame to the non-AP STA affiliated with the non-AP MLD. **Setting the field to 0 indicates that the AP has not determined when it will send a Disassociation frame to this STA or the AP affiliated with the AP MLD has not determined when it will send a Disassociation frame to the non-AP STA affiliated with the non-AP MLD. If the Disassociation Imminent field is (#17768)equal to 0, the Disassociation Timer field is reserved. The format of the Disassociation Timer field is shown in Figure 9-1154 (Disassociation Timer field format).**

https://slideplayer.com/slide/14828991/



Dec 2009 doc.: IEEE 802.11-09/1299r1

Behavior Changes (3):

Time before disassociation is at least 30 seconds

- **After the first BSS Transition Management Request frame sent to a non-AP STA with Disassociation Imminent field set to 1:**
  - The Disassociation Timer field is a number of TBTTs that is at least 30 seconds or "0" (disassociate time not decided yet)
  - AP keeps a countdown timer starting with the Disassociation Timer value (if it is not "0") or a number of TBTT at least 30 seconds (if Timer is "0")
  - Countdown timer is decremented by 1 with each beacon transmitted
  - In any subsequent BSS Transition Management Request frame sent to this non-AP STA, the Disassociation Timer shall be set to the value in the countdown timer

Submission Slide 15 Allan Thomson, Cisco Systems

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/

201015-802-11v-Basic-Service-Set-BSS-on-AireO.html

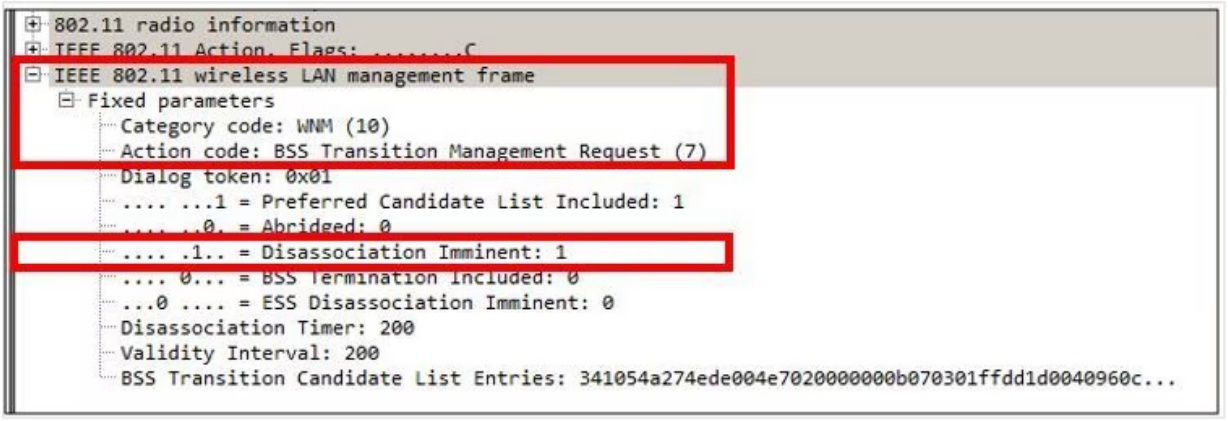
Disassociation Imminent

Within a BSS transition Management Request, Disassociation Imminent field can be added. This function is to disassociate the client after a period of time if the client does not re-associate to another AP.

When unsolicited optimized roaming request is triggered, the AP sends a BSS Transition Management Request to the client and wait for a certain period (time configured under Optimized Roaming Disassociation Timer), if the client does not roam to a better AP within that period of time, then the AP completes the disassociation of the client.

When Unsolicited Load Balance request is triggered, the AP sends a BSS Transition Management Request to the client and wait for a certain period (time configured under Disassociation Timer), if the client does not roam to a less congested AP within that period of time, then the AP completes the disassociation of the client.

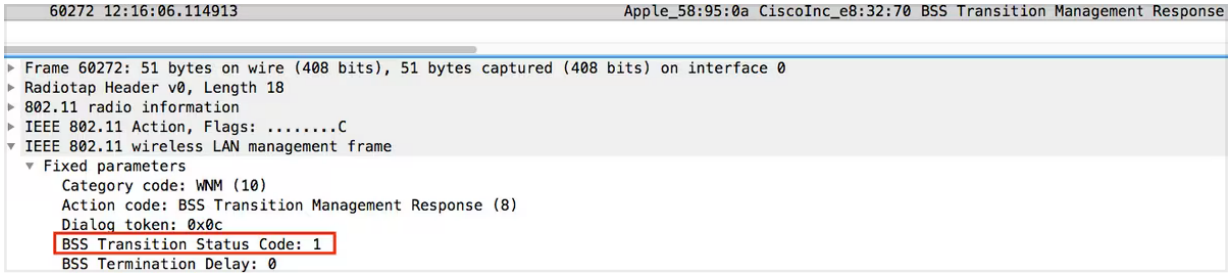
Example of a BSS transition management frame with Disassociation imminent enabled:



BSS Transition Management Response

After a wireless cleint has received a BSS Transition Management Request, it can or cannot send a BSS Transition Management Response. If the client transitions to another AP it sends it with status code Accept, but if it plans to stay on the same AP due to several reasons it sends it with status code Reject plus the reason of rejection.

Example of a BSS Transition Management Response frame

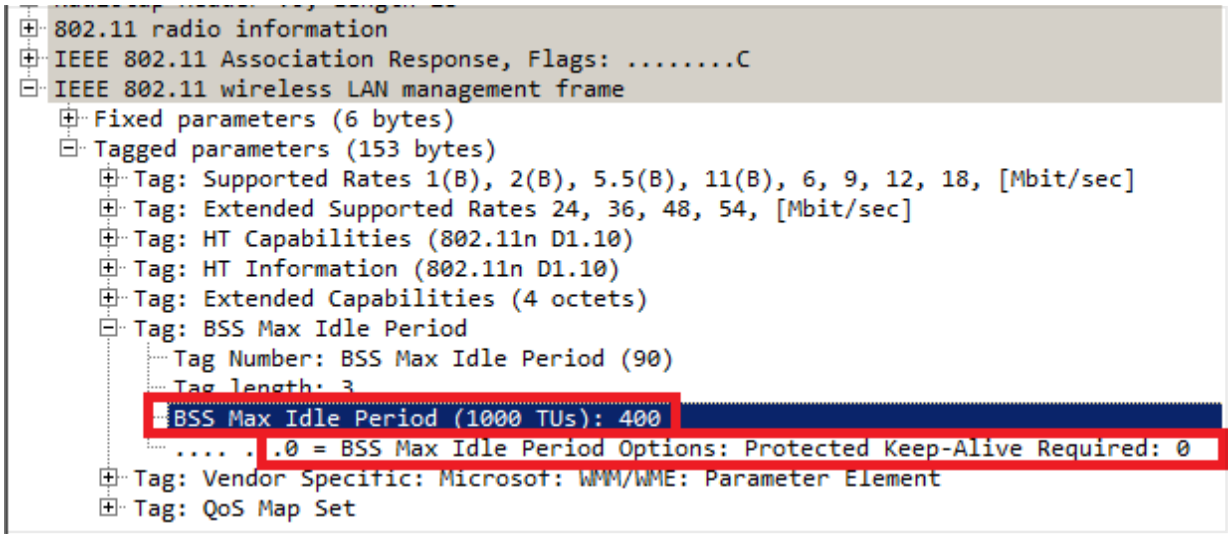


In this example the wireless client rejects the AP candidate list and does not roam to a different AP. The status code 1 shows the reason why the client leaves the ESS. For full list of status code definitions consult Table 8-253 of IEEE 802.11-2012.

BSS Max idle period: wlan.bss_max_idle.period

When an AP no longer receives frames from a wireless client for a certain period of time it assumes the client left the network and it disassociates it. The BSS Max idle period is the amount of time an AP can keep a client associated without have to receive any frame (client can remain sleep). This value is informed to the wireless client through the association and re-association response frame. This allows the clients to remain asleep for a longer time and save battery power.

BSS Max idle period only appears in association-response or re-association response frames



The BSS Max Idle Period is specified in units of 1000 TUs (Time units). Every time unit is equal to 1.024 milliseconds
Idle timeout = 1.024 x BSS Max Idle Period = X seconds
In the example frame:
Idle timeout = 1.024 x 405 = 414.72 seconds
If the Protected Keep-alive Required bit is set to 1, it means that the wireless client must send a RSN protected frame to the AP in order to reset the Idle Timer. If it is set to 0, as this example, the wireless client can send any type of frame (protected or unprotected) to reset the Idle timer at the AP.

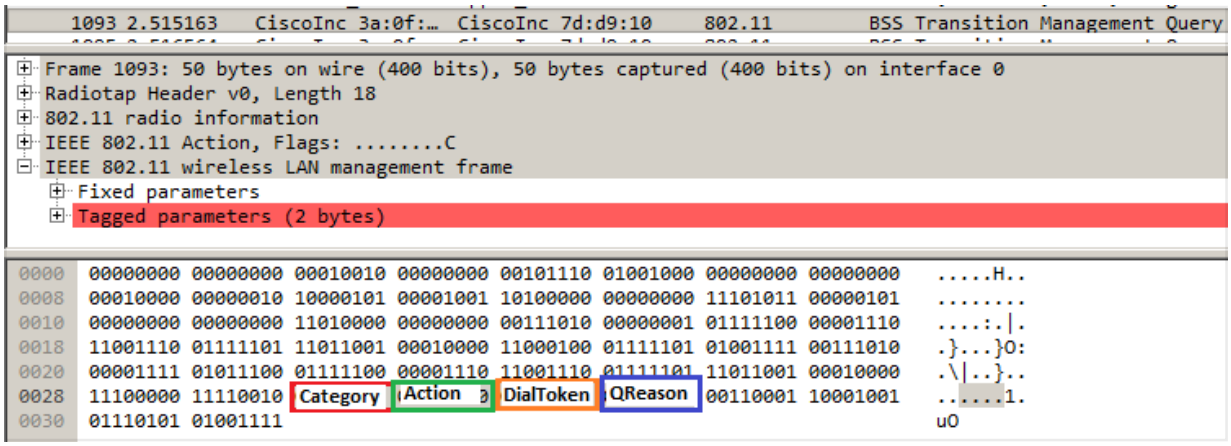
- **The Disassociation Timer indicates the time after which the AP will issue a Disassociation frame to this STA. The Disassociation Timer field is the number of beacon transmission times (TBTTs) until the AP sends a Disassociation frame to this STA. A value of 0 indicates that the AP has not determined when it will send a Disassociation frame to this STA**. If the Disassociation Imminent field is 0, the Disassociation Timer field is reserved. The format of the Disassociation Timer field is shown in Figure 8-476.

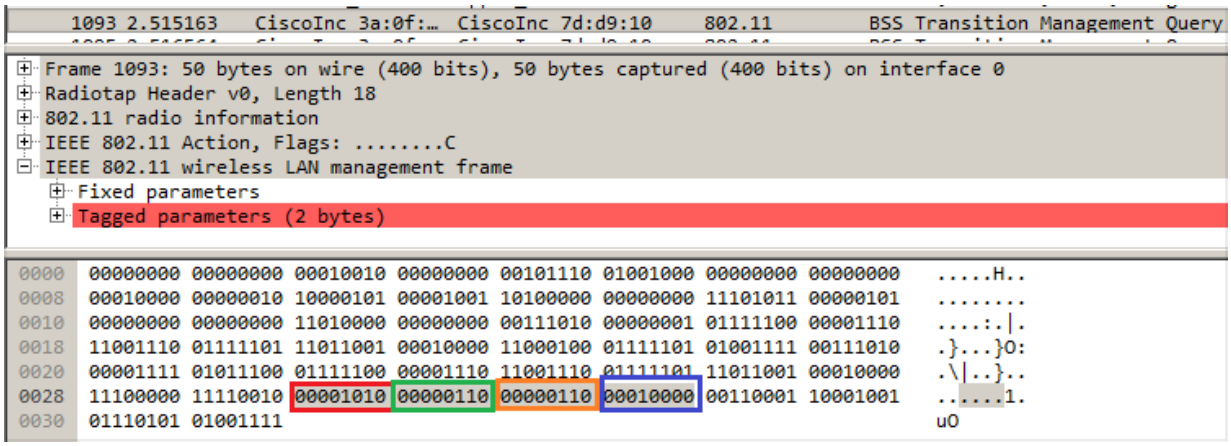
MENSAJES VISTOS EN EL BSS QUERY ENVIADO EN OCASIONES DESDE LOS DISPOSITIVOS CLIENTE AL AP.

olicited Request

Wireless client sends an 802.11v BSS Transition Management Query before they roam for a better option of APs to re-associate with.

Example of a 802.11v BSS Transition Management Query





QReason means BSS Transition Query Reason, which is the reason why the client requests the candidate AP list. In this example the client sent a reason 16, which correspond to Low RSSI. For full list of transition query reasons consult Table 8-138 of IEEE 802.11-2012.

Table 8-138—Transition and Transition Query reasons

Transition Reason value	Description
0	Unspecified
1	Excessive frame loss rates and/or poor conditions
2	Excessive delay for current traffic streams
3	Insufficient QoS capacity for current traffic streams (TSPEC rejected)
4	First association to ESS (the association initiated by an Association Request message instead of a Reassociation Request message)
5	Load balancing
6	Better AP found
7	Deauthenticated or Disassociated from the previous AP
8	AP failed IEEE 802.1X EAP Authentication
9	AP failed 4-Way Handshake

Table 8-138—Transition and Transition Query reasons *(continued)*

Transition Reason value	Description
10	Received too many replay counter failures
11	Received too many data MIC failures
12	Exceeded maximum number of retransmissions
13	Received too many broadcast disassociations
14	Received too many broadcast deauthentications
15	Previous transition failed
16	Low RSSI
17	Roam from a non-IEEE 802.11 system
18	Transition due to received BSS Transition Request frame
19	Preferred BSS transition candidate list included
20	Leaving ESS
21–255	Reserved

The Transition Result field contains the result of the attempted transition and is one of the status codes specified in Table 8-37 in 8.4.1.9.